



Time is on my side

Forging Wireless Timing Signals to Attack the NTP Server

Yuwei Zheng @HITB

Haoqi Shan @HITB

From: Qihoo360 Unicorn Team



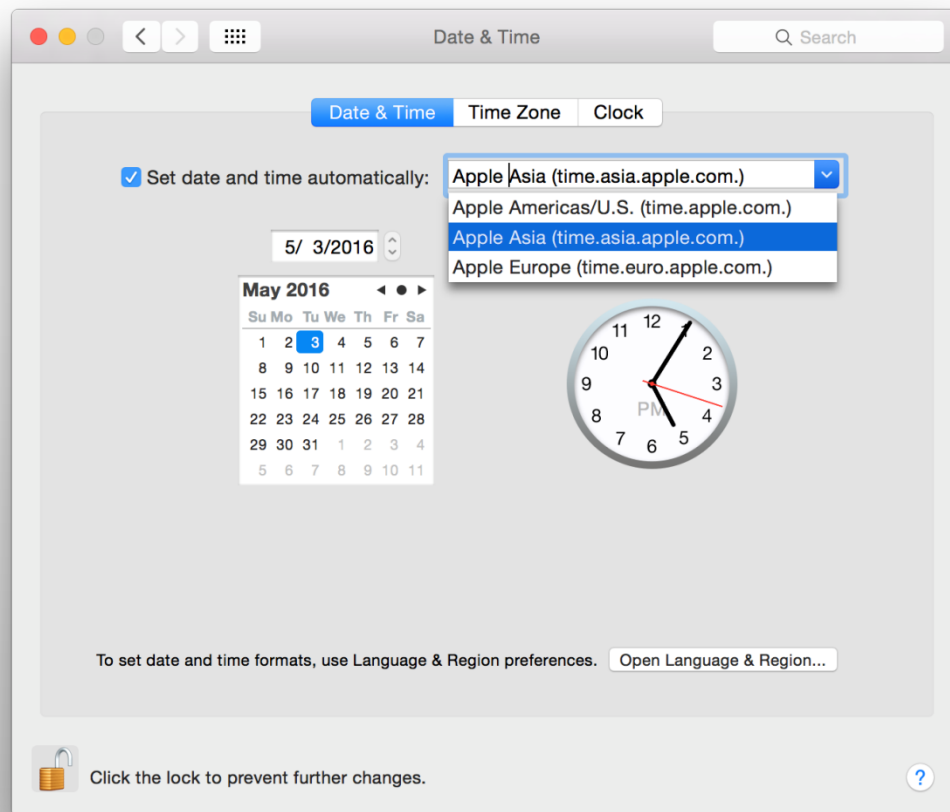
Main contents

- About the NTP server
- The NTP stratum mode
- The reference clock
- Forge radio clock signals
- Forge GPS clock signals
- Attack NTP server



About NTP server

- A server for computer to synchronize time.



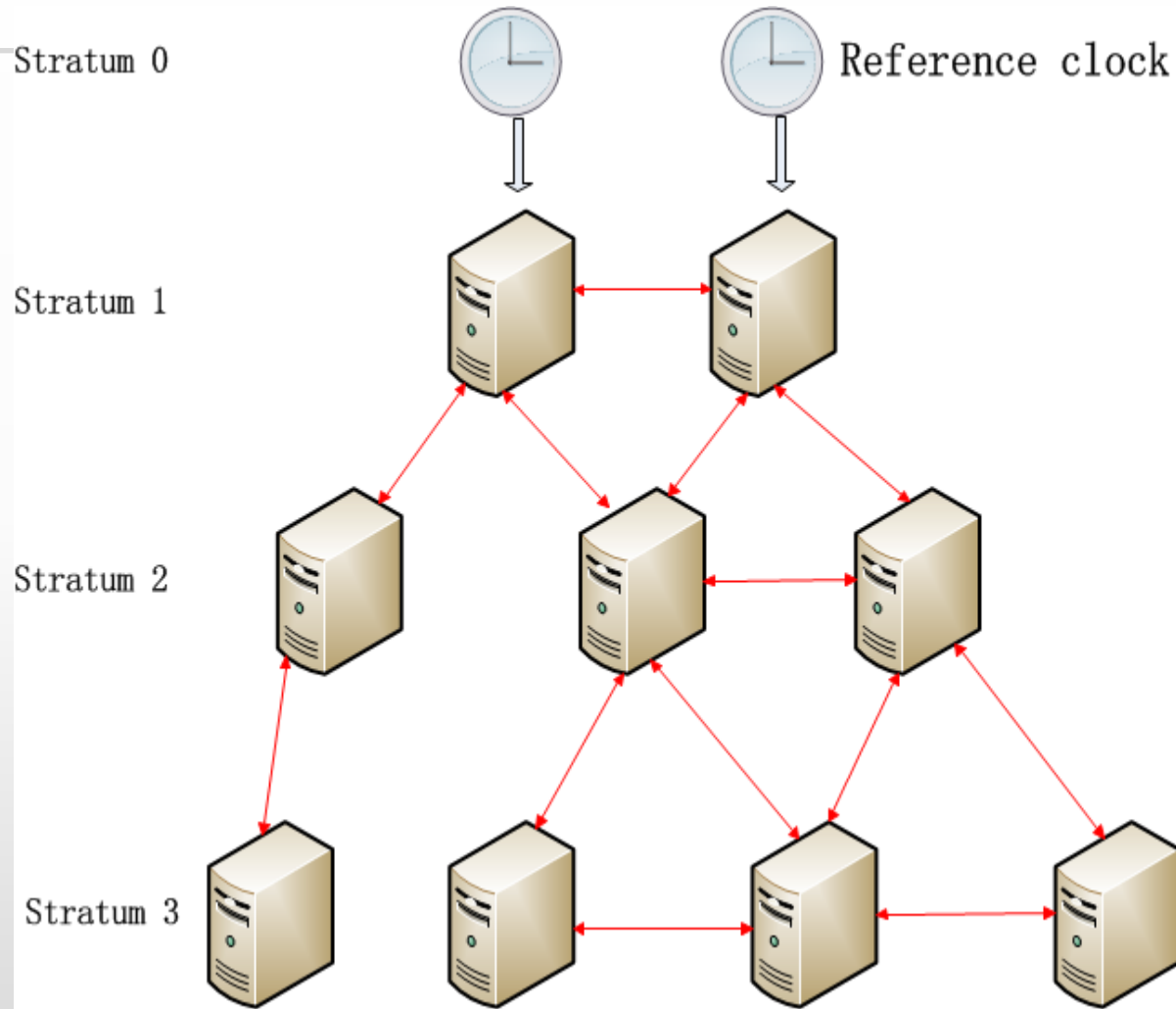
About NTP server

- Critical Industries that use NTP servers



The NTP stratum mode

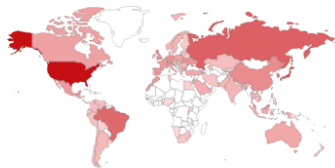
- Stratum 0
Reference clocks
- Stratum 1
Primary time servers
- Stratum 2
- Stratum 3
- ...
- Stratum 16



About the NTP server

- NTP servers are deployed with open source NTP v4

TOP COUNTRIES



United States	25,920
Japan	6,448
Russian Federation	3,308
Brazil	2,525
Korea, Republic of	1,597

TOP SERVICES

NTP	48,895
11265	4
49153	2
46081	2

Total results: 48,950

106.2.203.165

Priority of Fashion(Beijing)Information Technology

Added on 2016-05-19 02:04:56 GMT

🇨🇳 China, Beijing

[Details](#)

NTP

version: **ntpd** 4.2.6p5@1.2349-o Sat Nov 23 18:21:48 UTC 2013 (1)

processor: x86_64

system: Linux/2.6.32-504.e16.x86_64

leap: 0

stratum: 4

precision: -23

rootdelay: 61.944

rootdisp: 97.259

refid: 10.10.3.24

reftime: 0xdae79b11.7b9723db

clock: 0xdae79dc7.1aa99ad2

peer: 23575

tc: 10

mintc: 3

offs...

27% ↑ 13.9K/ ↓ 641K/

The reference clock

- Reference Clock Drivers in the open source NTP v4

Type 2 Deprecated: was Trak 8820 GPS Receiver

Type 3 PSTI/Traconex 1020 WWV/WWVH Receiver (WWV_PST)

Type 4 Spectracom WWVB/GPS Receivers (WWVB_SPEC)

Type 5 TrueTime GPS/GOES/OMEGA Receivers (TRUETIME)

Type 6 IRIG Audio Decoder (IRIG_AUDIO)

Type 7 Radio CHU Audio Demodulator/Decoder (CHU)

...

Type 39 hopf GPS/DCF77 6039 for PCI-Bus (HOPF_P)

Type 40 JJY Receivers (JJY)

Type 41 TrueTime 560 IRIG-B Decoder

Type 42 Zyfer GPStarplus Receiver

Type 43 RIPE NCC interface for Trimble Palisade

Type 44 NeoClock4X - DCF77 / TDF serial line

Type 45 Spectracom TSYNC PCI

Type 46 GPSD NG client protocol



The reference clock

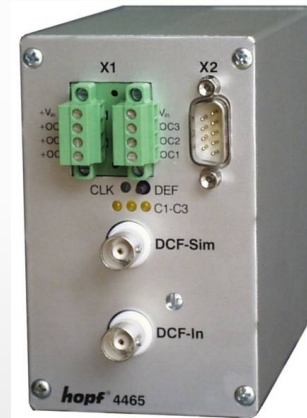
Why does the stratum-1 NTP server use radio clock and GPS ?

- Atomic clock, accurate, but expensive
- GPS
- radio clock



The reference clock

- Receiver cards supported by NTP V4



The reference clock

- Stratum 1 NTP server product for industrial using



The reference clock

- It supports DCF77, MSF, WWVB, and GPS

Internal receiver types for our LANTIME time servers

GPS satellite receiver

GLN - Combined GPS/GLONASS satellite receiver, can also be used for mobile applications

MRS - Multi Reference Source, different selectable synchronization sources

PZF (DCF77) receiver

IRIG timecode receiver

MSF time signal receiver (Great Britain)

WWVB time signal receiver (North America)

Meinberg Receivers



Low Profile GPS Clock (PCI Express)



PZF (DCF77 based) long wave time signal receiver

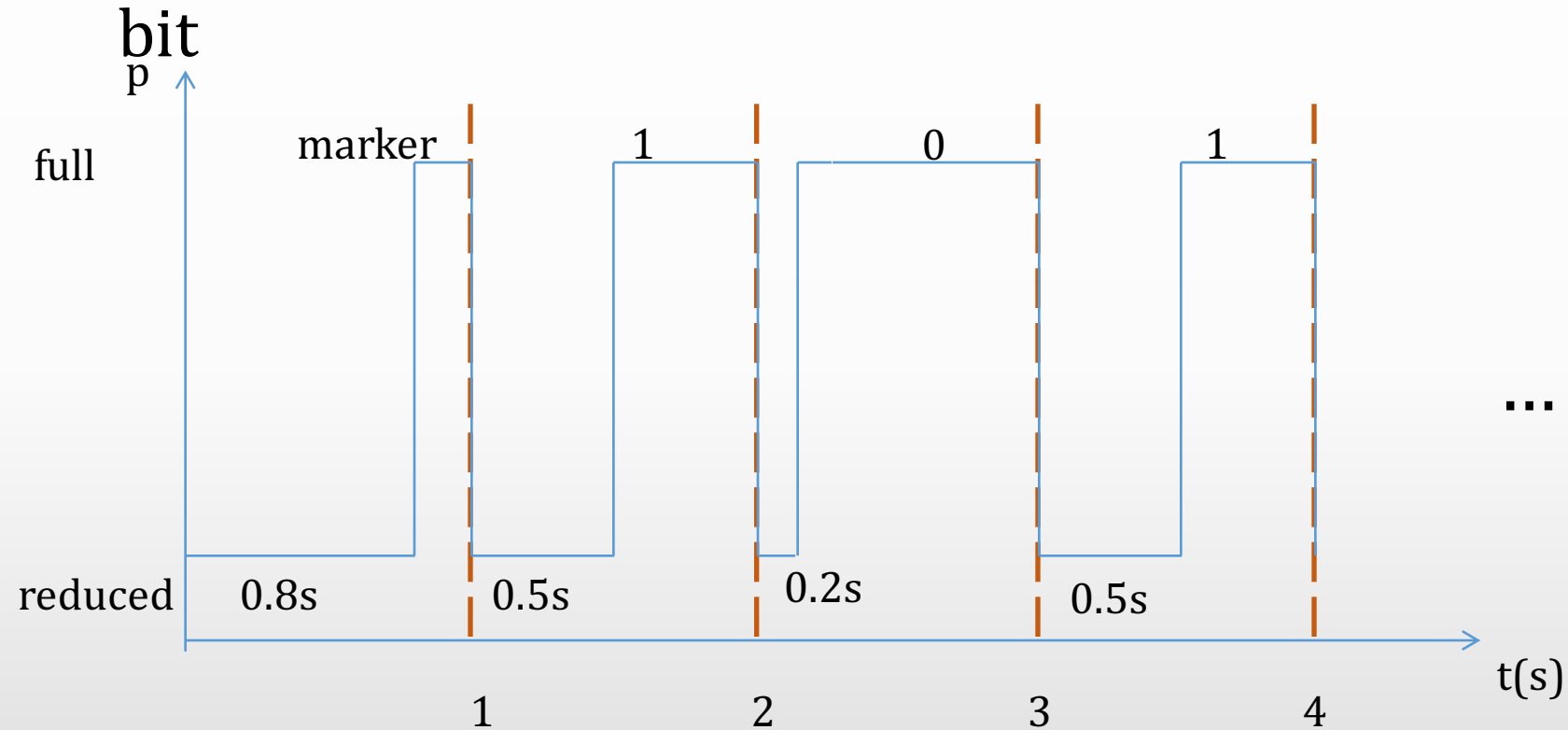
Forge long wave timing signals

- DIY a circuit to transmit radio clock signals support WWVB, JJY, DCF77, and MSF



WWVB encoding and modulation

- Different pulse width represent different data



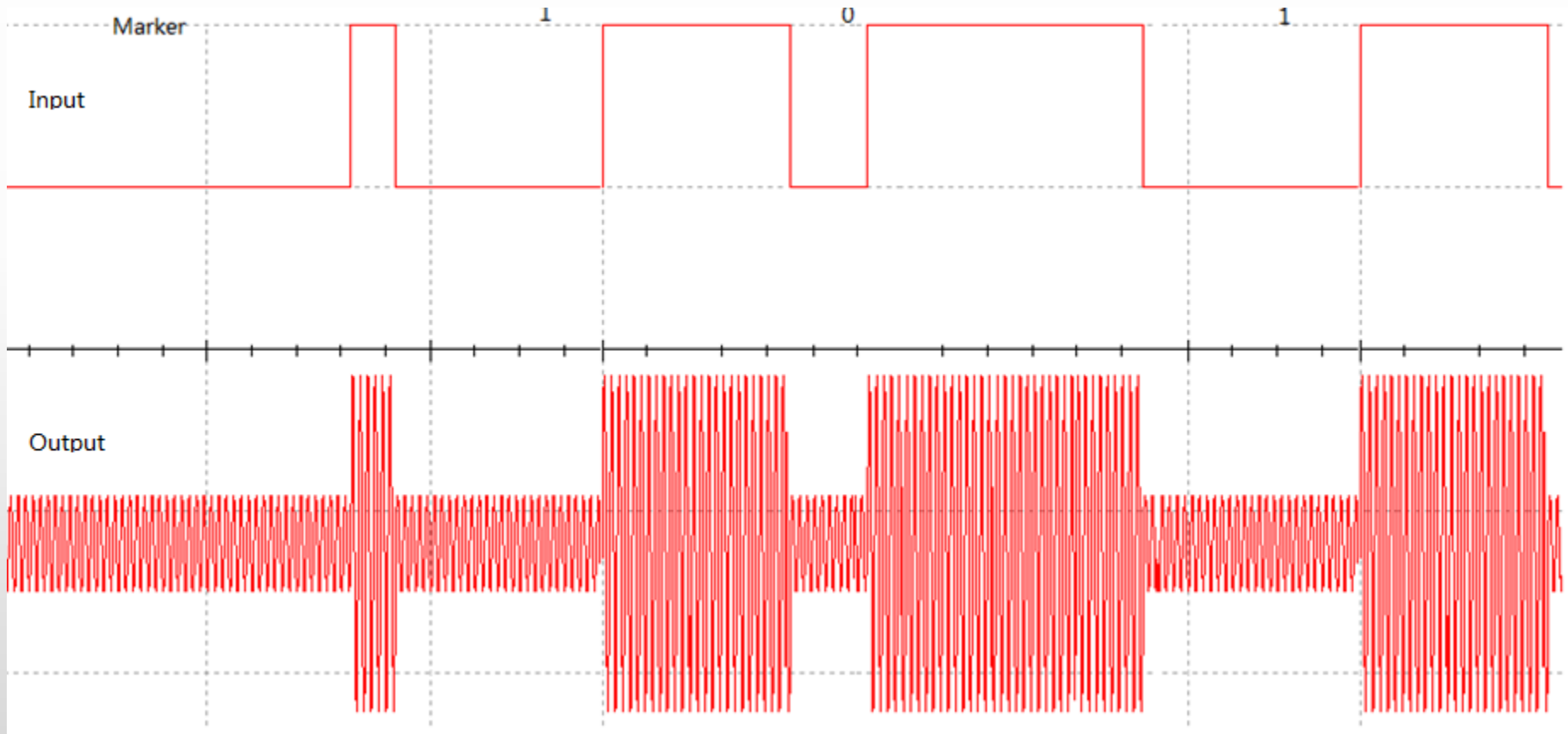
WWVB encoding and modulation

- 60Khz carrier



WWVB encoding and modulation

- ASK modulation



WWVB encoding and modulation

- The frame structure

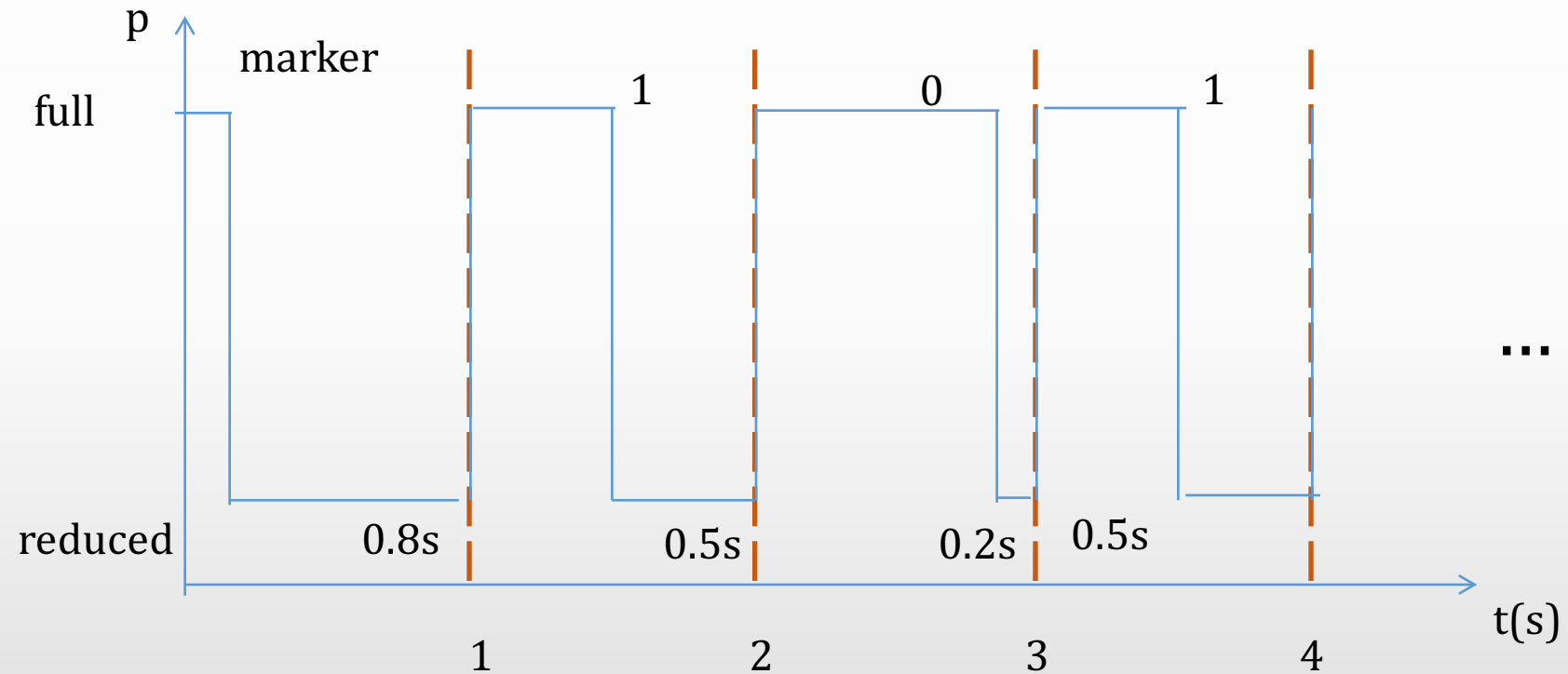
Bit	Weight	Meaning	Ex	Bit	Weight	Meaning	Ex	Bit	Weight	Meaning	Ex
:00	FRM	Frame reference marker	M	:20	0	Unused, always 0.	0	:40	0.8	DUT1 value (0-0.9 s). DUT1 = UT1-UTC. Example: 0.3	0
:01	40	Minutes (00-59) Example: 30	0	:21	0		0	:41	0.4		0
:02	20		1	:22	200		0	:42	0.2		1
:03	10		1	:23	100		0	:43	0.1		1
:04	0		0	:24	0	0	:44	0	Unused, always 0.	0	
:05	8	Day of year 1=January 1 365=December 31 (366 if a leap year) Example: 66 (March 6)	0	:25	80	Year (00-99) Example: 06	0	:45	80	Unused, always 0. [13]	0
:06	4		0	:26	40		1	:46	40		0
:07	2		0	:27	20		1	:47	20		0
:08	1		0	:28	10		0	:48	10		0
:09	P1	Marker	M	:29	P3	Marker	M	:49	P5	Marker	M
:10	0	Unused, always 0.	0	:30	8	Hours (00-23) Example: 07	0	:50	8	Leap year indicator	1
:11	0		0	:31	4		1	:51	4		0
:12	20		0	:32	2		1	:52	2		0
:13	10		0	:33	1		0	:53	1		0
:14	0	Unused, always 0.	0	:34	0	DUT1 sign. If +, bits 36 and 38 are set. If -, bit 37 is set. Example: -	0	:54	0	Leap second at end of month	0
:15	8		0	:35	0		0	:55	LYI		1
:16	4		1	:36	+		0	:56	LSW		0
:17	2		1	:37	-		1	:57	2		DST status value (binary): 00 = DST not in effect. 10 = DST begins today. 11 = DST in effect. 01 = DST ends today.
:18	1	1	:38	+	0	:58	1	0			
:19	P2	Marker	M	:39	P4	Marker	M	:59	P0	Marker	M

From <https://en.wikipedia.org/wiki/WWVB>



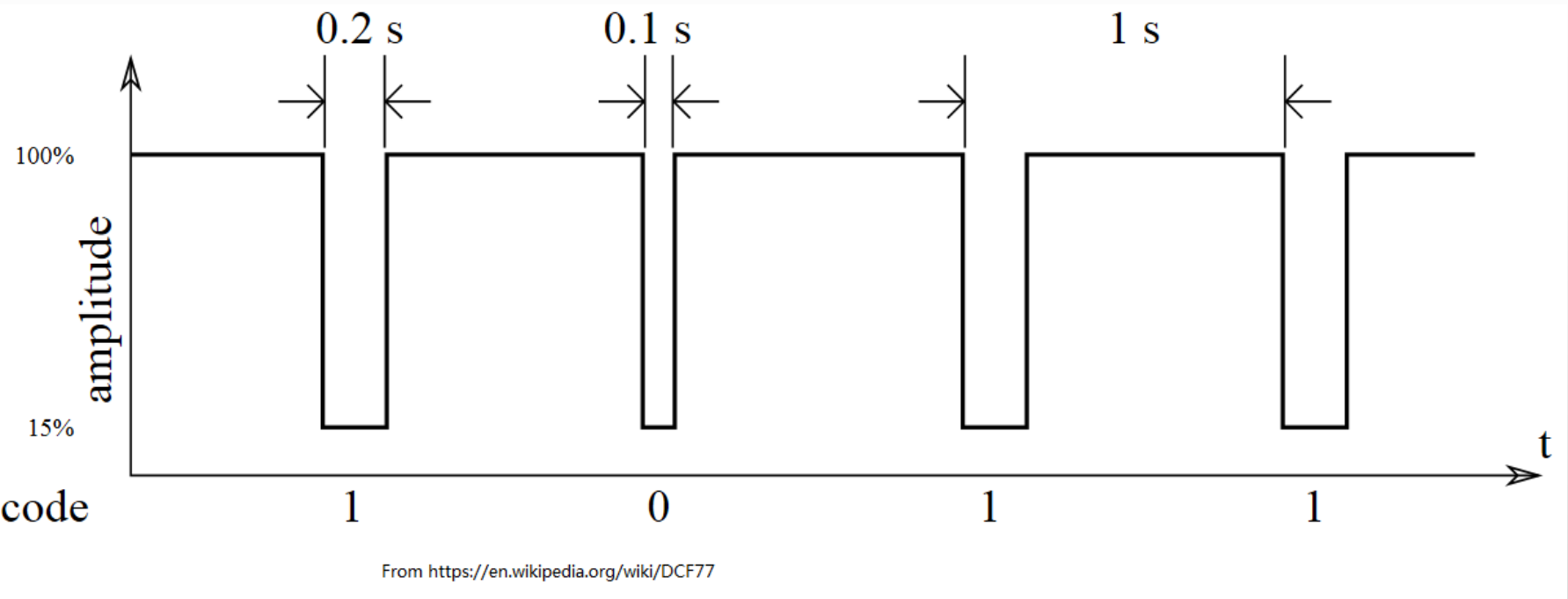
JJY encoding and modulation

Similar to the WWVB



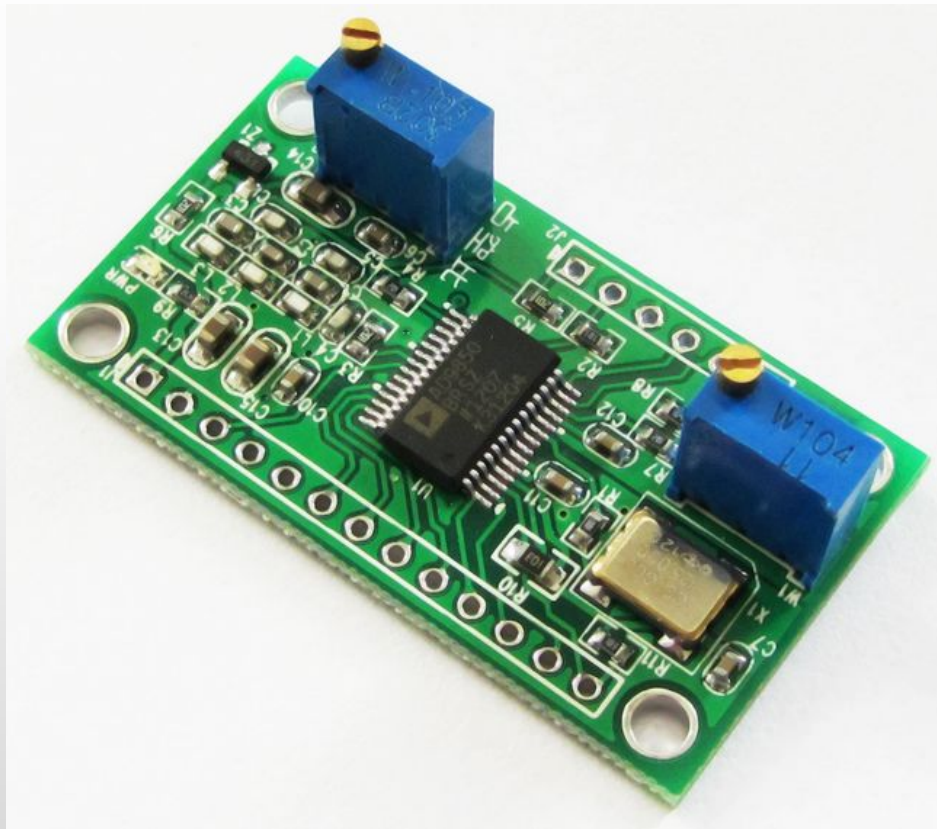
DCF77 encoding and modulation

- Similar to WWVB, it uses a 77.5hz carrier



Long wave timing signal transmitter

- Use ad9850 DDS module to generate the carrier



Long wave timing signal transmitter

- About AD9850 DDS module
supports to output 0-40Mhz wave
sends all radio clock signals with one circuit
- Use arduino to control ad9850
Ad9850 serial library for arduino
<https://github.com/F4GOJ/AD9850>

Long wave timing signal transmitter

- A simple JY transmitter

```
void sendMark() {  
    // Send high for 0.2 sec  
    DDS.setfreq(freq, phase);  
    delay(200);  
    // Send low for 0.8 sec  
    DDS.down();  
    delay(800);  
    return;  
}
```

Long wave timing signal transmitter

- A simple JY transmitter

```
void sendBit1() {  
    // Send high for 0.5 sec  
    DDS.setfreq(freq, phase);  
    delay(500);  
    // Send low for 0.5 sec  
    DDS.down();  
    delay(500);  
    return;  
}
```



Long wave timing signal transmitter

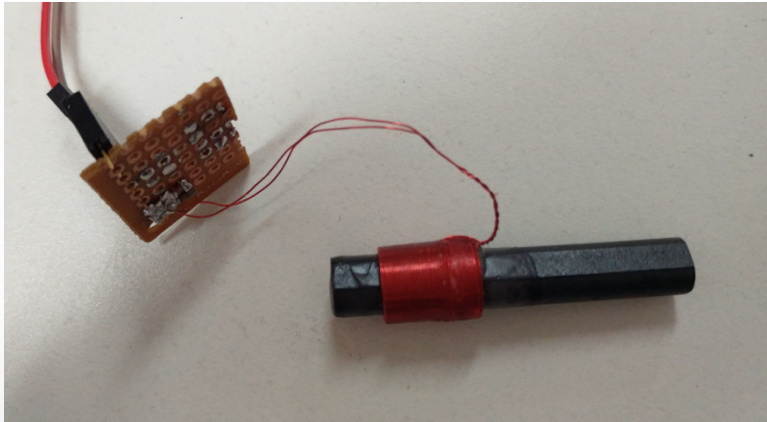
- A simple JY transmitter

```
void sendBitZero() {  
    // Send high for 0.8 sec  
    DDS.setfreq(freq, phase);  
    delay(800);  
    // Send low for 0.2 sec  
    DDS.down();  
    delay(200);  
    return;  
}
```



Long wave timing signal transmitter

- Get the antenna from an JY receiver



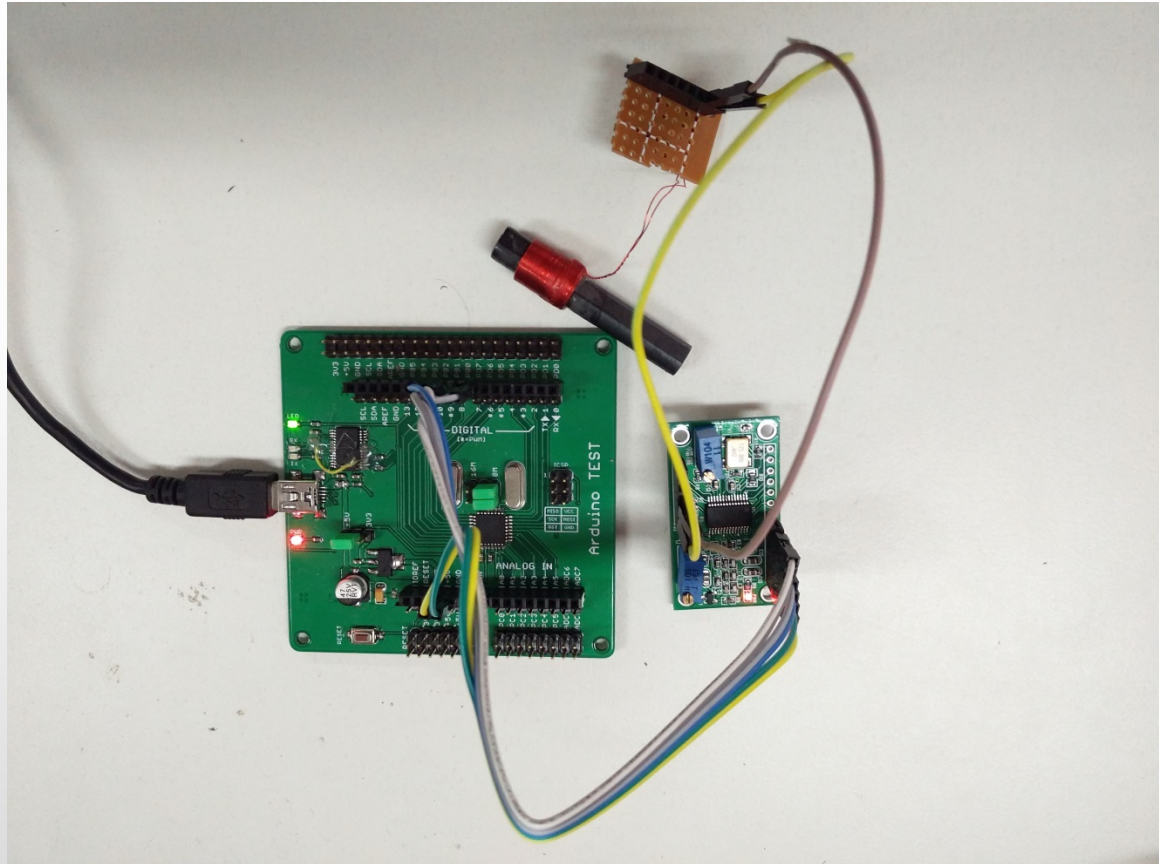
$$L = 1890\mu\text{H}.$$

$$f = \frac{1}{2\pi\sqrt{LC}}, \text{ for } 60\text{kHz carrier } C = 3.6\text{nF}$$

For the 77.5kHz carrier, $C = 2.2\text{nF}$

Long wave timing signal transmitter

- The whole circuit of the uniform transmitter



Long wave timing signal transmitter

- Long distance transmitter

Design a power amplifier with MOSFET IR540.

Attack GPS NTP receiver

- GPS receiver
- GPS tech briefing
- Generate GPS signal
- Have a try
- Upgrade attack algorithm



GPS receiver

- Multiply Connection
 - PCI
 - USB
 - Serial port

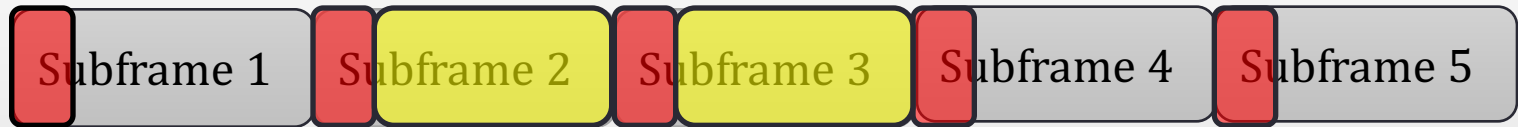
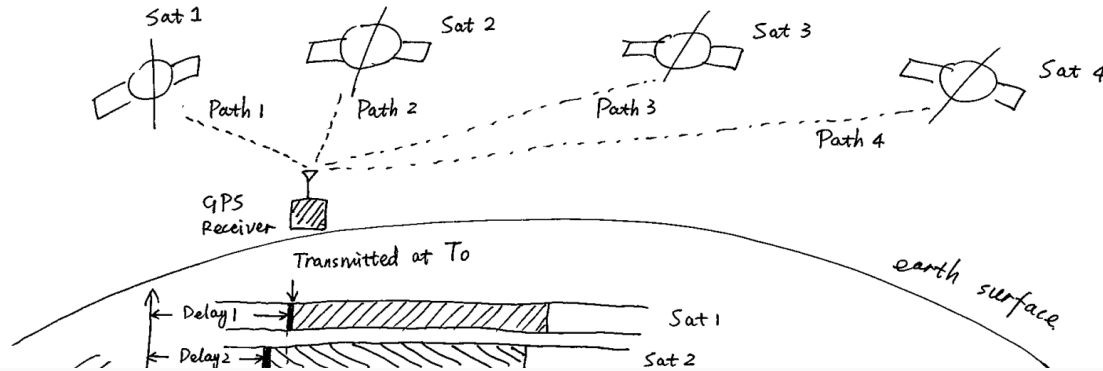


GPS tech briefing

- Complicated principle
- But doesn't matter, it's open-sourced
- Defcon23 "GPS Spoofing - Lin Huang"



GPS tech briefing



Time information

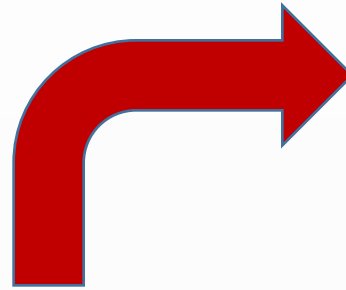
Ephemeris

Generate GPS signal

```
1  %*****
2  %名称:主函数
3  %功能:程序的入口函数
4  %作者:贾立伟
5  %时间:2014.07.11
6  %*****
7  clear;
8  clear global;
9  clc;
10 global SimGlobal;
11 global CT;
12 disp('-----');
13 set_time = Time(2016,05,16,12,0,0);
14 set_position = PVA;
15 set_position.pos.first = 36.206888; % Latitude
16 set_position.pos.second = -115.194569; % Longitude
17 set_position.pos.third = 100; % Height
18 init_sim(set_time,set_position);
19 disp('-----');
20
21 % % set datafile name
22 datafilename = 'test.dat';
23 %ephemeris_file = 'brdc0451.15n';
24 ephemeris_file = 'brdc3540.14n';
25
26 [SimGlobal.noeph,SimGlobal.aEphData]=readrinex(ephemeris_file);% read ephemeris data
27 SimGlobal.aSatData=selecteph;% select ephemeris data
28 load_almanac_data(SimGlobal.aSatData,CT.MaxSatNum);
29 load_ionospheric_data(SimGlobal.aSatData,CT.MaxSatNum);
30 satvisible;% decide which satellite is visible
31 % genmessage_wo_almanac;% generate telegraph without subframe 4&5 data
32 genmessage; % generate telegraph with subframe 4&5 data
33 channel_data = genchannel;
34 gensignal(channel_data,datafilename);
```



Have a try



```
ahwei@ubuntu: ~
GPS_NMEA(0) using '$GNRMC,094905.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*25'
^[[aGPS_NMEA(0) gpsread: 75 '$GNRMC,094906.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*26'
GPS_NMEA(0) processing 75 bytes, timecode '$GNRMC,094906.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*26'
GPS_NMEA(0) effective timecode: 2016-05-17 09:49:06
GPS_NMEA(0) using '$GNRMC,094906.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*26'
GPS_NMEA(0) gpsread: 75 '$GNRMC,094907.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*27'
GPS_NMEA(0) processing 75 bytes, timecode '$GNRMC,094907.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*27'
GPS_NMEA(0) effective timecode: 2016-05-17 09:49:07
GPS_NMEA(0) using '$GNRMC,094907.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*27'
GPS_NMEA(0) gpsread: 75 '$GNRMC,094908.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*28'
GPS_NMEA(0) processing 75 bytes, timecode '$GNRMC,094908.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*28'
GPS_NMEA(0) effective timecode: 2016-05-17 09:49:08
GPS_NMEA(0) using '$GNRMC,094908.900,V,3958.896372,N,11628.996008,E,0.000,0.000,051716,,E,N*28'
```



Panic

```
ahwei@ubuntu: ~
GPS_NMEA(0) effective timecode: 2016-05-17 09:46:31
GPS_NMEA(0) using '$GNRMC,094631.000,V,3958.878390,N,11629.036002,E,0.000,241.059,051716,,E,N*2B'
GPS_NMEA(0) gpsread: 76 '$GNRMC,094632.000,V,3958.877377,N,11629.028765,E,0.000,41.240,051716,,E,N*1F'
GPS_NMEA(0) processing 76 bytes, timecode '$GNRMC,094632.000,V,3958.877377,N,11629.028765,E,0.000,41.240,051716,,E,N*1F'
GPS_NMEA(0) effective timecode: 2016-05-17 09:46:32
GPS_NMEA(0) using '$GNRMC,094632.000,V,3958.877377,N,11629.028765,E,0.000,41.240,051716,,E,N*1F'
refclock_transmit: at 65 127.127.20.0
refclock_receive: at 65 127.127.20.0
event at 65 GPS_NMEA(0) 8024 84 reachable
refclock_receive: 0.000000
refclock_sample: n 43 offset -4527.334893 disp 0.000000 jitter 0.000091
clock_filter: n 1 off -4527.334893 del 0.000000 dsp 7.937545 jit 0.000001
select: combine offset -4527.334893432 jitter 0.000000954
event at 65 GPS_NMEA(0) 903a 8a sys_peer
clock_update: at 65 sample 65 associd 23393
event at 65 0.0.0.0 c417 07 panic_stop -4527 s; set clock manually within 1000 s
.
local_clock ret: -1
event at 65 0.0.0.0 c41d 0d kern kernel time sync disabled
ahwei@ubuntu:~$
```



Update attack algorithm

```
init_sim.m Find Results EphData.m
1 classdef EphData
2     properties
3         PRN;
4         sT GPSTime; weekno;
5         afc, af1, af2;
6         Iode;
7         Crs, Crc, Cus, Cuc, Cis, Cic;
8         dn, m0, ecc;
9         Asqrt;
10        Toe;
11        Omega0;
```

- Find GPSTime
- Replace it
- Re-ParityCheck



Setup an NTP server

- Setup an NTP server using JJY as clock source

```
server 127.127.40.0 mode 1 prefer  
fudge 127.127.40.0 flag1 stratum 0
```

Setup an NTP server

- This NTP server with JJY reference clock

```
server 127.127.40.0 mode 1 prefer
fudge 127.127.40.0 time1 0.110 stratum 0 flag1 0
driftfile /var/lib/ntp/ntp.drift
~
~
~
```

Setup an NTP server (JJY)

```
68 114996.951 192.168.0.56      192.168.0.3      NTP      90 NTP version 3, symmetric passive
+ Frame 68: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
+ Ethernet II, Src: Vmware_89:53:46 (00:0c:29:89:53:46), Dst: Vmware_ff:e8:8c (00:0c:29:ff:e8:8c)
+ Internet Protocol Version 4, Src: 192.168.0.56 (192.168.0.56), Dst: 192.168.0.3 (192.168.0.3)
+ User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
+ Network Time Protocol (NTP Version 3, symmetric passive)
  + Flags: 0x1a
    Peer Clock stratum: primary reference (1)
    Peer Polling Interval: 7 (128 sec)
    Peer Clock Precision: 0.000001 sec
    Root Delay:      0.0000 sec
    Root Dispersion: 7.9409 sec
    Reference ID: LF Radio JJY Fukushima, JP 40 kHz, Saga, JP 60 kHz
    Reference Timestamp: May 13, 2016 09:58:28.107047000 UTC
    Origin Timestamp: May 13, 2016 09:58:53.149374000 UTC
    Receive Timestamp: May 13, 2016 09:58:54.693199000 UTC
    Transmit Timestamp: May 13, 2016 09:58:54.693438000 UTC

0000  00 0c 29 ff e8 8c 00 0c 29 89 53 46 08 00 45 b8  ..). .... ).SF..E.
0010  00 4c e7 9a 40 00 40 11 d0 c2 c0 a8 00 38 c0 a8  .L..@.@. ....8..
0020  00 03 00 7b 00 7b 00 38 9b b4 1a 01 07 ec 00 00  ...{.{.8 .....
0030  00 00 00 07 f0 df 4a 4a 59 00 da e0 23 c4 1b 67  ....JJ Y...#.g
0040  72 6b da e0 23 dd 26 3d 70 a3 da e0 23 de b1 75  rk..#.&= p...#.u
0050  7e fd da e0 23 de b1 85 29 9c  ~...#... ).
```



Attack the NTP server

- Can we inject any time ?
The time offset must be less than 4 hours.

- Inject a time that is one hour slow than real time
Server crashed !!!

Attack the NTP server

- Can we inject any time ?

If the time offset is more than 1000s, the server will shutdown.

Attack the NTP server

- Can we inject any time ?
the offset > 1000s, require manually adjust

```
clock_filter: n 1 off -12696.443990 del 0.000000 dsp 7.937500 jit 0.000000
select: combine offset -12696.443990401 jitter 0.000000477
event at 1921 JJY(0) 904a 8a sys_peer
clock_update: at 1921 sample 1921 associd 40549
event at 1921 0.0.0.0 c217 07 panic_stop -12696 s; set clock manually within 1000 s.
local_clock ret: -1
event at 1921 0.0.0.0 c21d 0d kern kernel time sync disabled
shui@ubuntu: /etc 4 2 0x66
```



Root Dispersion

```
71 115210.747192.168.0.56      192.168.0.3      NTP      90 NTP Version 3, symmetric passive
⊕ Frame 71: 90 bytes on wire (720 bits), 90 bytes captured (720 bits) on interface 0
⊕ Ethernet II, Src: Vmware_89:53:46 (00:0c:29:89:53:46), Dst: Vmware_ff:e8:8c (00:0c:29:ff:e8:8c)
⊕ Internet Protocol Version 4, Src: 192.168.0.56 (192.168.0.56), Dst: 192.168.0.3 (192.168.0.3)
⊕ User Datagram Protocol, Src Port: 123 (123), Dst Port: 123 (123)
⊖ Network Time Protocol (NTP Version 3, symmetric passive)
  ⊕ Flags: 0x1a
    Peer Clock Stratum: primary reference (1)
    Peer Polling Interval: 6 (64 sec)
    Peer Clock Precision: 0.000001 sec
    Root Delay: 0.0000 sec
    Root Dispersion: 3.9445 sec
    Reference ID: LF Radio JJY Fukushima, JP 40 kHz, Saga, JP 60 kHz
    Reference Timestamp: May 13, 2016 10:01:40.112055000 UTC
    Origin Timestamp: May 13, 2016 10:02:26.514374000 UTC
    Receive Timestamp: May 13, 2016 10:02:28.509026000 UTC
    Transmit Timestamp: May 13, 2016 10:02:28.509575000 UTC

0000  00 0c 29 ff e8 8c 00 0c 29 89 53 46 08 00 45 b8  ..). .... ).SF..E.
0010  00 4c e7 9b 40 00 40 11 d0 c1 c0 a8 00 38 c0 a8  .L.@.@. ....8..
0020  00 03 00 7b 00 7b 00 38 50 7c 1a 01 06 ec 00 00  ...{.{.8 P|.....
0030  00 00 00 03 f1 cd 4a 4a 59 00 da e0 24 84 1c af  ....JJ Y...$....
0040  a8 22 da e0 24 b2 83 ae 14 7a da e0 24 b4 82 4f  ."$. ... .z.$..O
0050  8a c6 da e0 24 b4 82 73 8b d1                    ....$..s ..
```

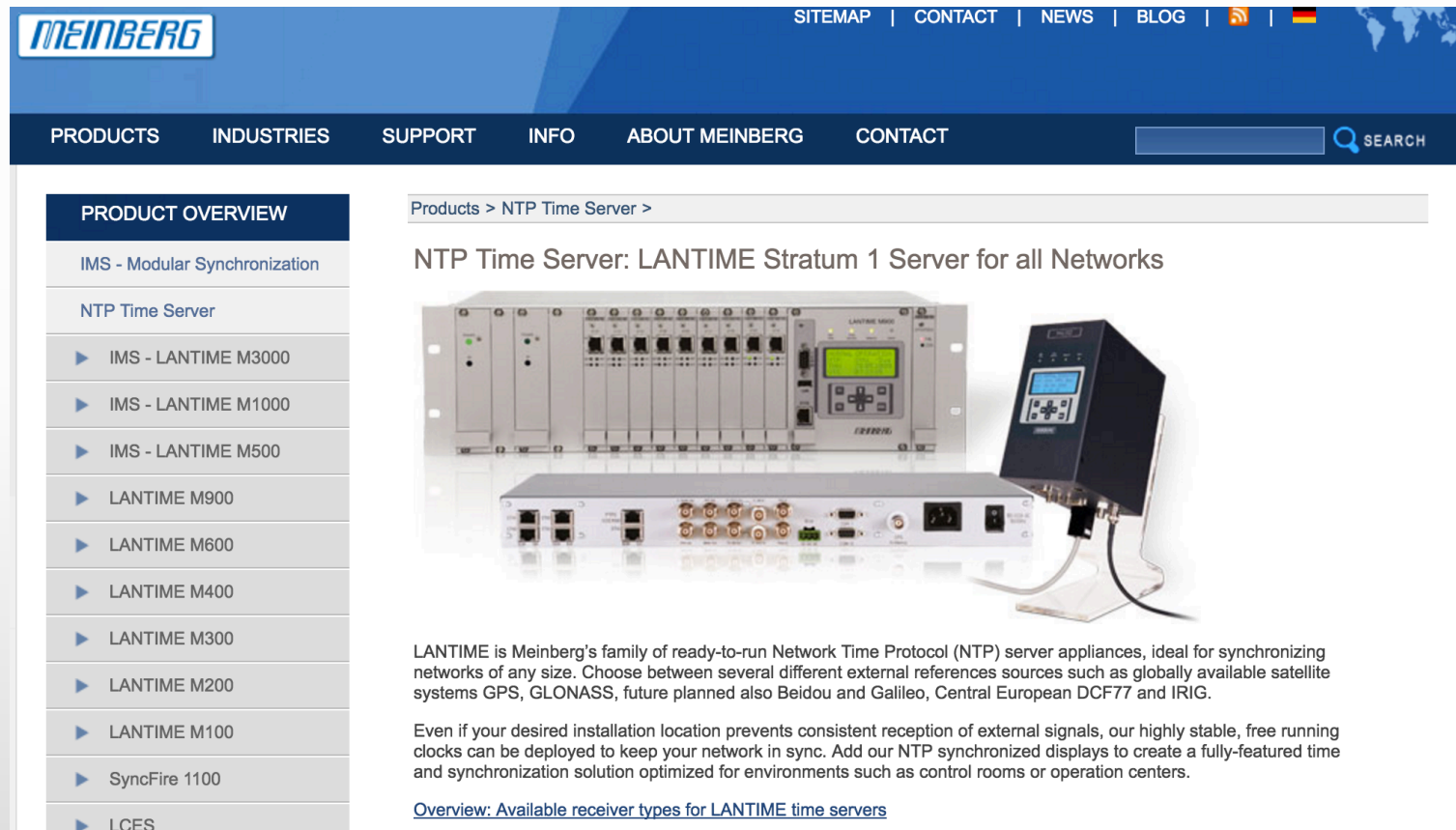
RFC5905



Attack Demo



Real Attack?



The screenshot shows the Meinberg website's product page for the LANTIME Stratum 1 Server. The header includes the Meinberg logo and navigation links for SITEMAP, CONTACT, NEWS, BLOG, and social media icons. The main navigation bar lists PRODUCTS, INDUSTRIES, SUPPORT, INFO, ABOUT MEINBERG, and CONTACT, along with a search bar. The left sidebar contains a 'PRODUCT OVERVIEW' menu with options like 'IMS - Modular Synchronization', 'NTP Time Server', and various LANTIME models. The main content area features the title 'NTP Time Server: LANTIME Stratum 1 Server for all Networks' and an image of the server hardware. Below the image, there is descriptive text about the LANTIME family of NTP servers and their capabilities, including a link to an overview of receiver types.

MEINBERG


SITEMAP | CONTACT | NEWS | BLOG | RSS | DE

PRODUCTS INDUSTRIES SUPPORT INFO ABOUT MEINBERG CONTACT

SEARCH

Products > NTP Time Server >

NTP Time Server: LANTIME Stratum 1 Server for all Networks



LANTIME is Meinberg's family of ready-to-run Network Time Protocol (NTP) server appliances, ideal for synchronizing networks of any size. Choose between several different external references sources such as globally available satellite systems GPS, GLONASS, future planned also Beidou and Galileo, Central European DCF77 and IRIG.

Even if your desired installation location prevents consistent reception of external signals, our highly stable, free running clocks can be deployed to keep your network in sync. Add our NTP synchronized displays to create a fully-featured time and synchronization solution optimized for environments such as control rooms or operation centers.

[Overview: Available receiver types for LANTIME time servers](#)

Real Attack?

Products

▼ Timing & Synchronization Systems

- Request a Quote
- Empower Channel Partners

▼ Products

- ▶ Clocks & Frequency References

▼ Time & Frequency Distribution

- ▶ GPS Instruments
- ▶ Modular Solutions

▼ Network Appliances / Servers

▼ Network Time Server / NTP Server

- SyncServer S650
- SyncServer S600
- Domain Time II
- Audit Server
- SyncServer S350+PTP
- SyncServer S350
- SyncServer S300

Network Time Server - SyncServer S200 (NTP)

Overview

Key Features

Order Information

Documents

The SyncServer S200 is being discontinued. The replacement model is the new [SyncServer S600](#).

Enterprise Class GPS Network Time Server (NTP)

Next Generation IT networks need accurate, reliable and secure time. Microsemi's high-performance Sync enterprise class GPS Network Time Server that supports the expanding technological requirements of large integrity of IT network accuracy, billing systems, electronic transactions, database integrity, VoIP quality, an applications.



Overview

The SyncServer S200 sets the standard for network time synchronization which is shared by Microsemi's c time servers.

Easy To Set Up and Maintain

SyncServers are the easiest to set up and maintain network time servers in the world. The front panel of the designed to quickly bring the server online with a few front panel keystrokes or DHCP. To fully configure the web interface or the step-by-step wizards for the most common operations.

Highly Robust and Secure

The S200 provides reliable and secure network synchronization technology by combining multi-port, high-s interfaces and versatile GPS timing receiver technology.

Real Attack?

SONOMA D12 Network Time Server GPS-Synchronized

Dual Gigabit Ports and 7500 NTP Packets / Second. [Read more...](#)

SONOMA D12 Network Time Server CDMA-Synchronized

Dual Gigabit Ports and 7500 NTP Packets / Second. CDMA antenna works indoors - even in your data center or colo. [Read more...](#)

PTP/IEEE-1588 Grandmaster Clock

The Sonoma can be used as a PTP/IEEE-1588 Grandmaster Clock by adding the PTP Option. [Read more...](#)

Sonoma N12 Network Time Server GPS-Synchronized

A Stratum 1 Time Server that uses GPS as its timing source. Rooftop & window-mount antenna kit included. [Read more...](#)



Real Attack?

- Sensitive & expensive

Ars Technica > Forums

New attacks on Network Time Protocol can defeat HTTPS and create chaos

POST REPLY ↘

realityofit

Wise, Aged Ars
Veteran

Registered: Feb 18, 2015
Posts: 113

True story. In 2008 I was working at a regional bank that had two data centers in different states. There was only one NTP server for the whole bank! I asked him what were the specs for the new NTP and the main frame support team reported that they were manually updating the time to keep it within a "seconds" requirements or standards for specific devices and none were currently defined and no one felt a



References

- “GPS Spoofing – Huang Lin”
- <https://www.eecis.udel.edu/~mills/ntp/html/refclock.html>
- http://www.sundgren.se/1-recreation/2-electronics/dcf77_simulator.htm
- <https://github.com/F4GOJ/AD9850>
- <https://github.com/sywcxx/gps-sim>



Thanks

- Any question?
- Feel free to contact us!

